United States v. Shacar
21-cr-30028-MGM
EXHIBIT “9”

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Vermont

U.S. DISTRICT COURT
DISTRICT OF VERMONT
FILED

2020 DEC -4 PM 3:12

CLERK

BY LAW
DEPUTY CLERK

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

54 Spruce St., Apartment 6, Burlington, VT

Case No. 2:20-mj-143-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein.

located in the _____ District of Vermont, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A(a)(2); 18 U.S.C. § 2252A(b)(1); 18 U.S.C. § 2252A(a)(5)(B); 18 U.S.C. § 2252A(b)(2)	Receipt of child pornography, possession of and access with intent to view child pornography, and attempt and conspiracy to commit those crimes.

The application is based on these facts:

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Seth Fiore, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/04/2020

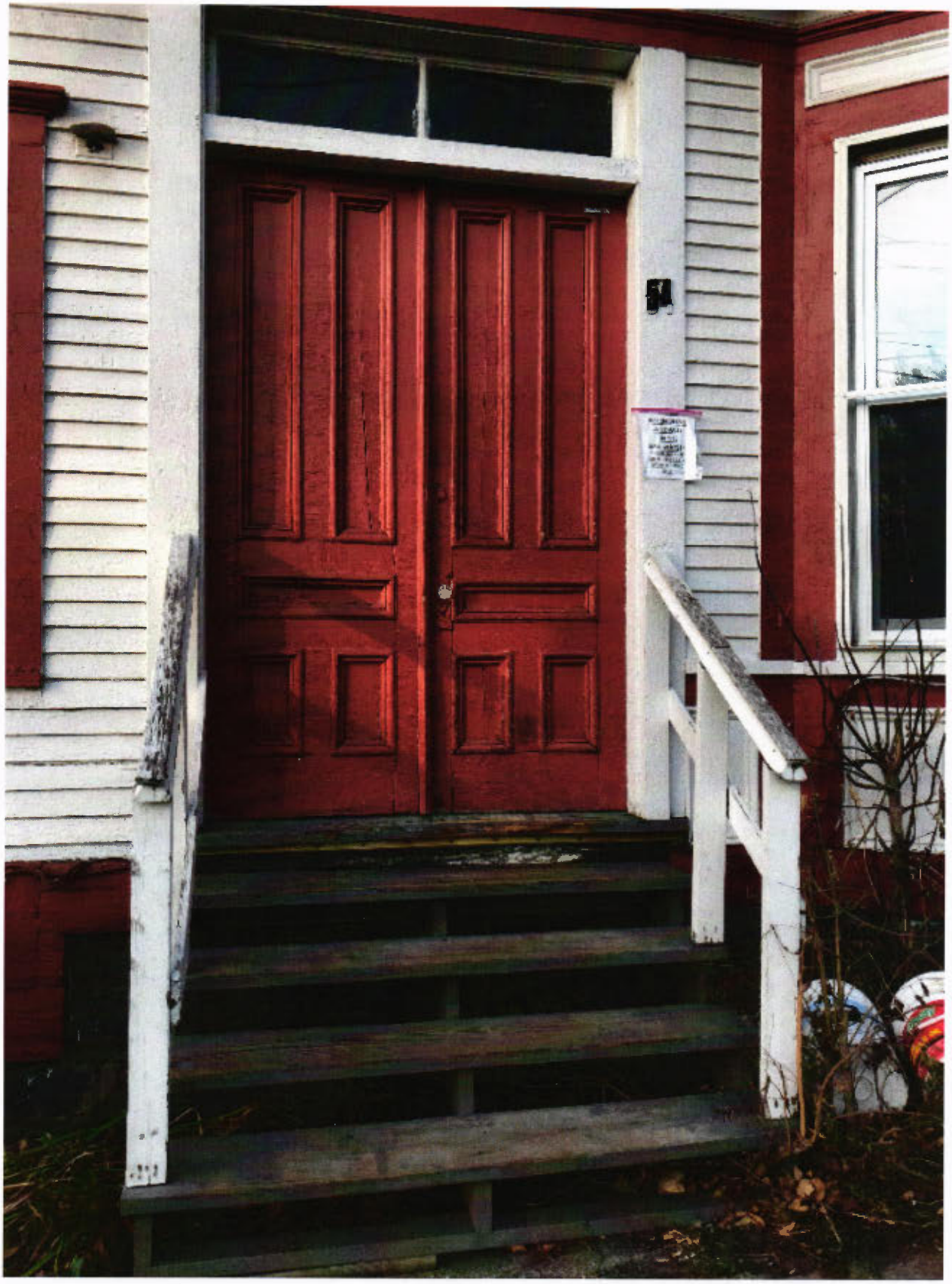
Judge's signature

City and state: Burlington, VT

Hon. John M. Conroy, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

The property to be searched is 54 Spruce St., Apt. 6, Burlington, Vermont, the TARGET PREMISES. The TARGET PREMISES is an apartment within a multi-level, multi-family dwelling. The building is painted white with red trim, with a main entryway on Spruce St. accessed by red doors. A black "54" over white is located aside from the red doors at the main entryway. Inside, apartments are identified by numbers affixed to or around doors. On the third floor, a black "6" is affixed to an apartment door.




NO SMOKING
ALLOWED
IN THE
HALLWAYS!!!

ATTACHMENT B

All property, records, and information, in any format, that constitute fruits, evidence and instrumentalities of violations of 18 United States Code §§ 2252A(a)(2) and (b)(1) (receipt of child pornography), and §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), and attempt and conspiracy to commit those crimes, ("the Target Offenses"), for the time period from April 12, 2019 to present (unless otherwise indicated), including, but not limited, to the following items:

1. Computers, cellular telephones and storage media, as defined below (hereinafter, "device(s)"), used as a means to commit the TARGET OFFENSES;

2. Child pornography, as defined in 18 U.S.C. § 2256(8), and/or visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

3. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors;

4. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the digital file(s), or that aid in the identification of persons involved in violations of the TARGET OFFENSES;

5. Records and information relating to the access, viewing or trafficking of child pornography, including correspondence and communications;

6. Records, information, and items relating to the occupancy or ownership of the TARGET PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

7. Records, information, and items relating to control and use of a Burlington Telecom internet subscription, including bills, mail envelopes, and payment information, including checking account, credit or debit card account information;

8. Records, information, and items relating to control and use of IP address 69.5.116.44, including bills, mail envelopes, and payment information, including checking account, credit or debit card account information;

9. For any device whose seizure is otherwise authorized by this warrant:

a. Items 2 to 8 above;

b. Links to child pornography or to online locations where child pornography is stored;

c. Records and information showing access to and/or use of websites and applications used to commit the TARGET OFFENSES;

d. Records of Internet activity related, including logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, and records of internet protocol addresses used;

e. Names, addresses, contact information or lists of names, addresses or contact information, in any format, of those who may have been contacted in connection with the TARGET OFFENSES;

f. Evidence indicating whether and/or when child pornography was accessed and/or viewed by any user of the device;

g. Evidence of who used, accessed, owned, or controlled the device;

h. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

i. Evidence of the lack of such malicious software;

j. Evidence indicating how and when the device was accessed or used, and evidence indicating the geographic location of the device when it was accessed or used;

k. Evidence of the attachment to the device of other electronic devices or similar containers for electronic evidence;

l. Evidence of counter-forensic programs;

m. Passwords and encryption keys, and other access information that may be necessary to access the device;

n. Evidence of applications used to communicate with other individuals;

o. Evidence of applications used to access and view child pornography and/or visual depictions of minors engaging in sexually explicit conduct;

p. Any and all stored data related to the access, receipt, exchange, or creation of child pornography and/or visual depictions of minors engaging in sexually explicit conduct;

q. Any stored data consisting of evidence of access to child pornography and/or visual depictions of minors engaging in sexually explicit conduct, including Internet logs, Internet browser histories, website bookmarks;

r. Any software used to access hidden-service-websites;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, network hardware, routers and modems, cellular telephones and digital cameras.

The term "storage media" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular telephones capable of storage, floppy

disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

"Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

"Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

Pursuant to Rule 41(e)(2)(B), it is authorized that electronically stored information may be imaged or copied. Consistent with Rule 41(e)(2)(B), the warrant is deemed executed once the subject computer has been physically seized, and that review of the contents of the subject computer is permitted at a later time.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Seth M. Fiore, a Special Agent of the Department of Homeland Security, Homeland Security Investigations, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of a premises – including computers contained therein – located at 54 Spruce St., Apartment 6, Burlington, Vermont (the "TARGET PREMISES"), as more fully described in Attachment A, which is incorporated herein by reference; and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, which is also incorporated herein by reference.
2. I have been employed as a Special Agent ("SA") of the Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") since October 2009 and am currently assigned to the Office of the Resident Agent in Charge, Burlington, Vermont. As part of my duties, I am authorized to investigate violations of the laws of the United States, including but not limited to criminal violations relating to the sexual exploitation of children, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of Title 18, United States Code ("U.S.C.") §§ 2422, 2423, 2251, and 2252A (and conspiracy and attempt to commit the same) and I am authorized by law to request a search warrant.
3. As an SA in the Burlington HSI office, I frequently participate in the execution of search warrants involving child exploitation and pornography, and I work closely with both HSI and state and local forensic computer specialists throughout these investigations and prosecutions. I have received training in the area of child exploitation and child

pornography and gained experience in this investigative field through my work in numerous federal investigations related to child exploitation and child pornography. I have participated in numerous investigations involving individuals suspected of sexual exploitation of children, child pornography, coercion and enticement, and transportation of minors, and have written, obtained and coordinated the execution of search and arrest warrants pertaining to individuals involved in those and other federal offenses. I have prepared numerous affidavits in support of applications for search and arrest warrants which have resulted in orders being issued by judges, including authorization to search premises and computers, including cellular telephones, which have led to the convictions of numerous defendants for violations of federal laws, including violations relating to child exploitation and child pornography. In addition to my training in the area of child pornography, I have had, in my investigative capacity, the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) on digital forms of media, including computer media.

4. The statements in this affidavit are based in part on information provided by federal agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, including foreign law enforcement agencies; information gathered from the service of administrative subpoenas and summonses; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by federal agents/analysts and computer forensic professionals; and my experience, training, and background as a Special Agent with HSI. This affidavit is intended to show merely that there is sufficient probable cause for the issuance of the search warrant, and does not set forth all of my knowledge about this matter.

5. As described in further detail below, a Tor-hidden-service-website that was dedicated to child exploitative images and child pornography (hereinafter, "the CP Website"), was

accessed on multiple dates from April 18, 2019 through May 5, 2019 by an Internet-connected computer using Internet Protocol ("IP") address 69.5.116.44. IP address 69.5.116.44 is owned and operated by Burlington Telecom, an Internet service provider. IP address 69.5.116.44 has been assigned to the customer account of William KEVE since November 6, 2018, and I confirmed with Burlington Telecom that, on November 18, 2020, it was still active. The physical address associated with the customer account and the IP address is 54 Spruce St., Apartment 6, Burlington, Vermont – the TARGET PREMISES and what I believe to be KEVE's home. On November 16, 2020, United States Postal Inspection Service electronically informed me that mail with the last name of Keve is delivered to 54 Spruce St., Apartment 6, Burlington, Vermont.

6. A public records report for William KEVE, accessed through Consolidated Lead Evaluation and Response ("CLEAR"), a public records database that can be accessed and searched over the Internet, indicated that KEVE has been associated with the TARGET PREMISES since November 2018.

7. As described herein, I believe that a user of the Internet account at the TARGET PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a hidden service website that operated on the Tor anonymity network. The website is described in the Probable Cause section of this affidavit and referred herein as the CP Website. There is probable cause to believe that a user of the Internet account at the TARGET PREMISES accessed the CP Website, as further described herein.

8. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 United States Code §§ 2252A(a)(2) and (b)(1) (receipt of child pornography), and §§ 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography), and attempt and conspiracy to commit those crimes, ("the

TARGET OFFENSES") have been committed at the TARGET PREMISES, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the TARGET PREMISES, described in Attachment A of this Affidavit. There is also probable cause to authorize the forensic examination of computers contained within the TARGET PREMISES for the purpose of identifying electronically stored data, particularly described in Attachment B.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachment B:

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

c. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order

to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text- based online communications such as Internet forums and email.

d. "Cellular telephone (or mobile telephone, or wireless telephone, or smartphone)" as used herein, is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other cellular telephones or traditional "land line" telephones. A cellular telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, cellular telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

e. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

f. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range

of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal- genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

k. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

The Tor Network

10. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

11. An IP address, as used herein, refers to a unique number used by a computer or other electronic device to access the Internet. An IP address (version 4) looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 01.234.01.234). Every computer or electronic device accessing the Internet must be assigned an IP address so that Internet traffic sent from or directed to that device may be properly directed from its source to its destination (akin to a telephone call being routed using a telephone number subscribed to a certain handset). Most ISPs, for example Burlington Telecom, control a certain range of IP addresses. IP addresses may be "static," if an ISP assigns a user's electronic device (e.g. a modem, router or computer) a particular IP address that is used each time the device accesses the Internet. IP addresses may also be "dynamic," meaning that the ISP assigns a different unique number to a device each time the device accesses the Internet using the ISP's service. ISPs typically maintain logs of the IP addresses assigned to users during sessions on particular dates and times.

12. The CP Website, further described below, operated on the Tor network, a computer network available to Internet users designed specifically to facilitate anonymous communication over the Internet. The Tor network is included in an area of the internet commonly referred to as the "dark web" because it is not publicly indexed on popular

search engine websites (e.g., Google). The Tor network attempts anonymity by routing Tor-user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through relay computers, traditional IP-address-based identification techniques are not effective.

13. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.[1] The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

14. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

15. Tor may be used to access open-Internet websites like www.justice.gov. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor

[1] Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

node from observing the content (but not the routing information) of other Tor users' communications. Similarly, this encrypted traffic can prevent law enforcement from observing the content of communications, even when judicially authorized (e.g., Title III authorization).

16. The Tor Project maintains a publicly available frequently asked questions ("FAQ") page, accessible from its website, with information about the Tor network, https://support.torproject.org/faq (last accessed on November 20, 2020). Within those FAQ, the Tor Project advises Tor users that it is possible for some entities to see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the network does not render a user's communications totally anonymous.

17. The Tor Network also makes it possible for users to operate websites, such as the CP Website, that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Hidden-services-websites often attempt anonymity to prevent their host servers from being seized or shut down by governments or law enforcement, whether or not they are used for illegal purposes (e.g., sites that host dissident political speech, sites that host child pornography). Like other websites, hidden-services-websites are hosted on computer servers that communicate through IP addresses. However, hidden-services-websites have unique technical features that attempt to conceal the computer server's location.

18. Unlike standard open-Internet websites (those publicly available on the surface web addresses using common Internet browsers like Microsoft Internet Explorer, e.g., justice.gov), a Tor-based web address is comprised of a series of at least 16, and as many as 56, algorithm-generated characters, for example, "asdlk8fs9dflku7f," followed by the suffix ".onion" (i.e., asdlk8fs9dflku7f.onion). Ordinarily, investigators can determine the IP

address of the computer server hosting an open-Internet website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing (akin to a phone book for registered open-Internet websites). Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor-hidden-service-website computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden service users can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden-service-website.

19. Hidden-service-websites on the Tor Network are not "indexed" by search engines – such as Google – to anywhere near the same degree as websites that operate on the open-Internet. Accordingly, it is much more difficult to perform a Google-type search of Tor-hidden-service-websites than it is to search open-Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and child pornography websites they operate) must willfully seek out these websites and therefore keep, maintain, and use directory sites that advertise the web addresses of hidden-service-websites that contain child exploitation related content. Users utilize those directory sites to identify new hidden-service hosts of web forums, chat sites, image galleries, and file sharing pertaining to the sexual exploitation of children. While in operation, the web address for the CP Website was listed on one or more of these directory sites advertising hidden-service-websites dedicated to the sexual exploitation of children.

The CP Website

20. The CP Website was an online chat site whose primary purpose was to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. The CP Website started operating in approximately 2018 and appeared to cease operating in 2020.

21. On the front page of the site, the CP Website stated that the site was intended for users to "post links with good photos and videos" depicting "[o]nly GIRLS 4 to 14 years [old]." The site allowed users to engage in online chat with other users, either within chat rooms that were openly accessible to any user of the site, within rooms only accessible to particular users, or in one-to-one chats between two (2) users. Child pornography images and videos were trafficked through this chat site via the posting of web links within chat messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos were stored in order to download these images and videos. The CP Website provided its users with information about particular file hosting websites where users could upload digital files so that the files could then be shared, via links, with other users on the CP Website.

22. Entry to the site was obtained through free registration, as described below. On the registration page, it read, among other things, "No hurtcore, No gore, No zoo, No death, No toddlers." In my training and experience, "zoo" refers to pornography depicting bestiality, and "hurtcore" is a genre of child pornography that depicts violence, gore, torture, humiliation, or children in pain and distress. In addition, the registration page of the CP Website expressly contemplated the sharing of videos between members. Language on that page read, "Post links with good photos and videos (preview is required!)."

23. In order to pass through the registration page and gain access to the actual content of the CP Website, a prospective user must create a "Nickname" and a password which must be entered along with a Captcha. A "Captcha" is a randomly generated series of characters

designed to ensure that users of a website are human beings and not bots or other automated processes. Users are not required to enter any personally identifiable information, such as true names, emails, or phone numbers. The users may also pick a color for their posts (or one was randomly generated) and click "enter chat."

24. Upon initially creating a user account on the CP Website, a user was assigned the status of "Guest." As an unregistered user, the user receives the following message upon log in: "As it looks like you are not registered you may check our rules by sending to me word rules. There also will be some additional explanation of how to use this feature. News! We added feature of forum. Access by button at the bottom or just by this link: forum. this should make you be more happy of getting this message on entrance." Unregistered or "Guest" users could access the CP Website postings including postings that shared child pornography images.

25. In order to fully register an account, the user would need to obtain a promotion from "Guest" to "Registered Guest," which was done at the discretion of the CP Website staff. After an individual was promoted to a registered user account on the CP Website, a user must log in to that user account with the appropriate user-generated password in order to communicate via that user account on the CP Website. The CP Website users may register, log into, and access the CP Website through that user account using any computer or electronic device that was configured to use Tor routing/software.

26. As is common on these types of sites, the CP Website was administered and moderated by select CP Website users referred to as "Members" on the site. These users were promoted at the discretion of the site leadership. Promotions appeared to be made based on an individual's active participation on the site. Once promoted to a Member position, those users enforced the rules and assisted in the management of the site. That included controlling user membership using the "ban" and "kick" functions (which can limit or

eliminate a user's participation or account), promoting within the ranks of users, and moderating the public chatroom for content and user behavior.

27. CP Website Members periodically re-posted standard messages to the public chatroom of the CP Website iterating rules and procedures of the CP Website. For example, on or about May 28, 2019, a Member on the CP Website posted "CHAT RULES" in the public chatroom. That post contained statements in both Russian and English which included but was not limited to, "Follow the requests of the Members," "No hurtcore, No gore, No zoo, No death, No toddler," "Only GIRLS 5 to 13 years. Any language allowed," and "For RG (registered guests) the photo archive is available (the "links" button)."

28. Also on or about May 28, 2019, a Member posted "SECURITY INFORMATION" in the public chatroom. That post contained statements in both Russian and English which included but was not limited to the following:

- Set the Security Slider to HIGH Security Level
- Do Not Download if you are not using Encryption or Tails OS
- Read these manuals: □ Tails Guide & Tor Security Guide □
- Do Not Share any Identifying Information & NEVER Trust Anybody!
- Windows & OS X/MacOS are not safe for On topic
- Save files only to Encrypted Storage
- Windows Leaves traces you cannot clean without a Full disk wipe
- Linux offers Full Disk Encryption, Tails is Amnesic
- use VeraCrypt to create Hidden Encrypted Containers
- Open files when Offline to lower risk of malicious file causing trouble
- LEA & Antis are known to pose as parents and kids to trick you into revealing information to them, suspect everyone is LEA.
- LEA could be running this or any site at any time

- Always be conscious your messages may not be private

- Be Careful Paying for Anything, Bitcoin is not Anonymous by default!

29. When a user posted in the open chat, other users could see the name of the poster, what was posted and what time it was posted. Images posted to the site could be categorized or "tagged" by users based upon the image theme or characteristics. Those tags aided users in searching for specific types of content.

30. There was also an advertisement in the middle of the CP Website chat screen stating, "VISIT OUR SITES" and it featured four (4) links to other Tor sites. Each site had a short description along with a link to the Tor web address for the site. The descriptions stated: "Forum for boy-and girlovers" with a link to another website; "Chat for boylovers" – with a link to another website; "Girls pedo portal", and "only Ru". Based on my training and experience, I am aware that the reference to "only Ru" means that site is only for Russian speakers. Further, based on my training and experience, it is apparent that those websites were associated with each other.

31. The CP Website provided users with numerous links to image hosts where users could upload their digital images. For instance, on November 2, 2018, a CP Website user posted a hyperlink of a .jpeg file that linked to an image of a prepubescent girl having her underwear pulled down and a male penis resting on her inner thigh near her exposed vagina. In another instance, on March 1, 2019, a CP Website user posted a hyperlink of a .jpg file that linked to an image of a prepubescent female bent forward on what appeared to be a wooden chair with her back towards the camera. She was wearing a black and red skirt and no underwear. The female's anus and vagina were prominently exposed for the camera. Her face was turned to the side making it partially visible through her hair. The female had no pubic hair, was small in stature, and young facial features. Also, on May 27, 2019, a CP Website user posted a hyperlink to a .jpg image depicting a nude prepubescent female laying on a bed.

The image only showed the male's torso and upper leg from the side. The adult male was pushing his erect penis into the female's mouth.

32. Postings to the CP Website that were publicly available to any registered user at the time of posting were captured and archived for law enforcement review. Over 1,200,000 messages were posted on the CP Website between March 2018 and March 2020 when the site appeared to go offline. FBI SAs have accessed and downloaded child pornography files via links that were posted on the CP Website, in an undercover capacity.

33. A foreign law enforcement agency (herein referred to as "FLA") described the website as facilitating "the sharing of child sexual abuse and exploitation material, stipulating only girls aged 5 – 13.[2] Users were required to enter a username and password but these were only valid for that single login session" and provided further documentation naming the website as the CP Website, which the FLA referred to by its actual name.

34. While acting in an undercover capacity and observing the approximately over one (1) million files of suspected child pornography, law enforcement was able to access and download suspected child pornography files via links that were posted on the CP Website while it was still operating. Review of such postings included (but are not limited to) the following images within the CP Website:

a. **1556381394.jpg**: This is an image file which depicts what appears to be a fully nude, prepubescent, preteen girl laying on a comforter or bedding with her arms crossed, with a nude adult male touching his mostly erect penis and partially penetrating the girl vaginally.

b. **1544966953192.jpg**: This is an image file which depicts what appears to be a fully nude, prepubescent, preteen, very young girl sitting on a nude adult male's stomach, while the adult male appears to be lying on his back. The young girl's right hand is gripping the adult

[2] The range of ages of images in chats within the CP Website, as was reposted to the public chatroom by a CP Website Member, as described by FBI special agents appears to have been narrowed by one (1) year on each end of the age range from what FLA viewed on the front page of the CP Website, as described in paragraph 21.

male's erect penis. In the background appears to be two more naked girls, similar in age to the young girl sitting on the nude adult male's stomach.

c. **1544967068710.jpg**: This is an image file which depicts what appears to be a fully nude, prepubescent, preteen girl lying on a bed and looking up at a nude adult male sitting on the same bed with an erect penis. There appears to be a second, fully nude, prepubescent, preteen girl sitting on the same bed and looking at the camera which captured the image. In the background, there appears to be a third nude, young girl sitting up on the same bed.

Information Received from a Foreign Law Enforcement Agency

35. I am aware that U.S. and foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor-hidden-service-websites, including the CP Website described herein. These websites are globally accessible. Exploitative Tor-hidden-service-websites, and their users, can be located anywhere in the world. Due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where geographically a particular exploitative Tor-hidden-service-website or user of that website is located. Accordingly, when a law enforcement agency obtains evidence that such an exploitative Tor-hidden-service-website or user may be located in another country, it is common practice for that law enforcement agency to share information with law enforcement agencies in the countries where the exploitative website site is located, or the country where the offender appears to reside, in accordance with the laws of each country.

36. In or around August 2019, an FLA known to U.S. law enforcement and with a history of providing reliable, accurate information in the past, notified U.S. law enforcement that FLA had determined that on April 18, 2019 at 14:45:04 Coordinated Universal Time ("UTC"), IP

address 69.5.116.44 was used to access online child sexual abuse and exploitation material via the CP Website which FLA named and described. FLA provided approximately six (6) additional dates and times IP address 69.5.116.44 was used to access the CP Website.

37. FLA is a national law enforcement agency of a country with an established rule of law. There is a long history of U.S. law enforcement sharing criminal investigation information with FLA, and FLA sharing criminal investigation information with U.S. law enforcement. This occurs across disciplines, including the investigation of crimes of children exploitation and child pornography. FLA advised U.S. law enforcement that it had obtained information related to access to the CP Website by IP address 69.5.116.44, as well as other IP addresses, through an independent investigation that was lawfully authorized in FLA's country pursuant to its national laws. FLA further advised U.S. law enforcement that FLA had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain the IP address information. U.S. law enforcement personnel did not participate in the investigative work through which FLA identified the IP address information provided by FLA.

38. I am aware through my training and experience and consultation with other U.S. law enforcement agents that, as part of this investigation, leads and information provided by FLA regarding IP addresses that FLA advised were associated with access to Tor hidden-service child exploitation-related web and chat sites have:

a. led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse;

b. led to the seizure of evidence of child pornography trafficking and possession; and

c. been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.

39. As described herein, the CP Website could not generally be accessed through the traditional Internet (i.e., using common web browsers including Microsoft Internet Explorer). Certain efforts needed to be employed to access the CP Website, including software installation and seeking out hidden-service-websites hosting child pornography. Only a user who had installed the appropriate Tor software on the user's computer (which may include smartphone cellular telephones) could access the CP Website. Even after connecting to the Tor network, a user would have to find the correct 16-or-56-character web address of the CP Website in order to access it. Hidden-service-websites on the Tor network are not "indexed" by search engines - such as Google - to anywhere near the same degree as websites that operate on the open-Internet. Many are not indexed by popular public search engines at all. Accordingly, it is much more difficult to perform a Google-type search of hidden-services-websites than it is to search open-Internet websites for particular content of interest. Users interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain, and use directory sites that advertise the web addresses of hidden-services-websites that contain child exploitation related content. Those directory sites also operate via the Tor network. Users utilize those directory sites to identify new Tor-hidden-service forums, chat sites, image galleries, and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (e.g., boys, girls, hurtcore). They also contain clickable hyperlinks to access those hidden sites and, as with other Tor-hidden-service-websites and, a user must find the

16-or-56 character web address for a directory website in order to access it. While it operated, the CP Website was listed on one or more of such directories of hidden sites advertising services dedicated to the sexual exploitation of children.

40. I am also aware - through HSI's consultation with agents from the Federal Bureau of Investigation ("FBI") - that the review of detailed user data related to another Tor-hidden-service child pornography website found that it was exceedingly rare for a registered website user to only access that website once and never return. FBI review of user data from that particular website found that less than two hundredths of one percent (0.02%) of user accounts registered an account on the Tor-hidden-service-website, accessed a message thread on the website, and then never returned to the website or never again logged in to the same account. Simply put, users of hidden-service child pornography websites seek out and find those sites that they enjoy and then return for continued use of the site. And where one child pornography website "goes down" and is no longer accessible (e.g., it is seized or disrupted by law enforcement), users of hidden-service child pornography websites will then seek out other similar sites, using directories and other means.

41. Accordingly, based on my training and experience and the information articulated herein, because accessing the CP Website required numerous affirmative steps by the user - including downloading Tor browser software, accessing the Tor network, seeking out the hidden-service web address for the CP Website, and then connecting to the CP Website via a Tor browser, it is extremely improbable that any user would simply stumble upon the CP Website, a hidden website, without understanding the clear purpose of the CP Website - to host and provide access of exploitative child pornographic material to users of the CP Website.

42. Accordingly, I submit that there is probable cause to believe that, based on the reasons described in this affidavit, any user who accessed the CP Website has, at a minimum,

knowingly and willfully accessed the CP Website with intent to access, view, and possess child pornography, and conspired with other individuals to do so.

IP Information Associated with the TARGET PREMISES

43. According to publicly available information, IP address 69.5.116.44 – used to access the CP Website on dates ranging from April 18, 2019 through May 5, 2019 – was determined to be owned and operated by ISP Burlington Telecom and subscribed to and used by KEVE.

44. On or about November 21, 2019, an administrative subpoena was served on Burlington Telecom for information related to the use of the IP address on April 18, 2019 at 14:45:04 UTC; April 24, 2019 at 17:27:15 UTC; April 26, 2019 at 14:42:31 UTC; April 27, 2019 at 15:14:17 UTC; May 1, 2019 at 19:17:20 UTC; May 3, 2019 at 13:53:39 UTC; and May 5, 2019 at 14:27:39. Burlington Telecom provided the following subscriber details:

- **Account Number**: 196022675
- **Name**: William Keve
- **Address**: 54 Spruce St., Apt. 6, Burlington, VT 05401
- **Active Date**: November 6, 2018
- **Account Status**: Active
- **Phone**: 802-734-5860
- **Email**: WILLKEVE@gmail.com

45. In order to ensure KEVE's continued subscription to the account, I contacted Burlington Telecom and received, on November 18, 2020, an email from Burlington Telecom stating that account 196022675 was still active, KEVE was the subscriber, and the address was the same.

46. In sum, IP address 69.5.116.44 accessed the CP Website on April 18, 2019; April 24, 2019; April 26, 2019; April 27, 2019; May 1, 2019; May 3, 2019; and May 5, 2019. The IP address was assigned to KEVE's account then as it is now. I believe KEVE's Burlington

Telecom Internet account and the IP address associated with the TARGET PREMISES were used to access the CP Website.

USE OF COMPUTERS FOR CHILD PORNOGRAPHY

47. I have had training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:

a. Computers and digital technology, including cellular telephones and removable storage media, are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four (4) functions in connection with child pornography: production, communication, distribution, and storage.

b. Cellular telephones with cameras can take and save photographs or videos as a digital file that can be directly transferred to another computer via an Internet connection. Photos and videos taken on a cellular telephone may be stored to internal device memory or a removable memory card in the cellular telephone. Photos and video can also be transferred from computers to cellular telephones. The memory in cellular telephones, whether internal memory or removable memory cards, is often large enough to store thousands of high-resolution photographs or videos.

c. The ability of computers and cellular telephones to store images in digital form make the devices ideal repositories for child pornography. Storage media is any physical object upon which computer data can be recorded. The size of available memory for electronic storage media used in personal devices has grown tremendously within the last several years. Electronic storage media of various types - to include computer internal hard drives, external hard drives, CDs, DVDs, USB "thumb," "jump," or "flash" drives, and removable micro storage drives that can be contained inside of a cellular telephone (e.g., a Micro-SD card) - can store thousands of images or videos at very high resolution. It is extremely easy

for an individual to take a photograph or a video with a camera-bearing cellular telephone, and then save it (or any other files on the device) to any one of those media storage devices. Similarly, it is extremely easy for an individual to download a photograph or a video from a website and save it to internal device memory, or save or copy it (or any other files on the computer) to any one of those storage media. Some storage media, now not much bigger than the size of a small coin, can easily be concealed and carried on an individual's person. Cellular telephones, carried on an individual's person, act as electronic storage media themselves.

d. The Internet affords individuals several different venues for accessing, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

e. Individuals may also use online resources to store and retrieve child pornography, including services offered by Internet cloud storage providers (e.g., Google, Apple iCloud, Dropbox) and Internet email providers (e.g., Google Gmail, Yahoo! (Oath), and Microsoft Hotmail), or using the Tor network as described above. Online service providers allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage or email account from any computer with access to the Internet. However, even in cases where online storage is used, in most cases evidence of child pornography can also be found on the user's personal computer or cellular phone, as those devices can be used to access the online storage.

f. As is the case with most digital technology, a computer used for online communication can save or store communications and data. Storing this information can be intentional (e.g., saving an e-mail as a file on the device or saving a web address in "bookmarked" files). Digital information can also be retained unintentionally, with traces of the path of an electronic communication automatically stored in many places (e.g., temporary files). In

addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" (e.g., thumbnail photographs) in a web cache and history files of the web browser used.

48. Through my experience and training, and that of other HSI Special Agents, the following traits and characteristics are generally found to exist in cases involving individuals who collect images of child pornography, including digital images:

a. The majority of individuals who collect child pornography are individuals with a sexually-motivated attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

b. The majority of individuals who collect child pornography often seek out likeminded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact also helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, websites, mobile applications, email, email groups, bulletin boards, Internet chat programs, newsgroups, instant messaging, and other similar platforms.

c. Individuals who collect child pornography often collect and maintain points of contact to access and receive child pornography. In the digital context, individuals often maintain names, online user names, and addresses (including email addresses, web addresses and URLs) of persons who have advertised or otherwise made known on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral or exchange, or a means to trade, access or receive child pornography. These contacts may be maintained in personal devices (computers and cellular telephones) as saved

communications (e.g., message threads in an application or text messages), contacts, digital notes, bookmarks, word or text files, of in other digital formats.

d. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections from discovery, theft, and damage. I know from training and experience that such individuals have been known to maintain possession of their child pornography for years, or even decades. Collections are almost always maintained in the privacy and security of their homes or other secure locations, including personal devices, computers and cellular telephones. As described herein, as computing power has increased and the price of memory and storage has decreased, it is quite easy for individuals to maintain gigabytes of data containing thousands of images of child pornography.

CASE PROGRESSION AND PROBABILITY OF EXISTING CONTRABAND

49. According to FLA, the CP Website was last accessed by IP address 69.5.116.44 in the spring of 2019. Once United States law enforcement received the IP address from FLA, FBI issued an administrative subpoena, dated November 21, 2019, to Burlington Telecom. Once FBI received data related to IP address 69.5.116.44 from Burlington Telecom, it relayed data to HSI's Special Agent in Charge office in Boston, Massachusetts. After conducting precursory record checks, HSI Boston referred the investigation to HSI Burlington. On or around October 15, 2020, the investigation was assigned by HSI management to your affiant.

50. It is probable that computers located at the TARGET PREMISES will reveal evidence of commission of the TARGET OFFENSES, including evidence of a Tor browser and ongoing access to hidden-service-websites dedicated to child pornography. It is also probable that evidence of past storage of child pornography and past access to child pornography will be found. Forensic analysis of computers found at the TARGET

PREMISES are likely to find files and data 19-months old, or older, and this forensically recovered data from computers can reveal relevant evidence of an individual's commission of the TARGET OFFENSES.

51. Digital images and videos can easily and quickly be transferred between computers and storage media. Storage of these images, as described below, could occur to the memory of the computer used to access the Tor browser and hidden-service-websites, to discs or removable storage media, or to cloud-based storage solutions. Evidence of access to hidden-service-websites dedicated to child pornography could be readily apparent in computer logs and histories, or can be forensically recovered a computer's cache, as described below. Where computers are upgraded or replaced, it is now common for data and files to be transferred automatically from an "old" computer to a "new" computer (e.g., an Apple computer automatically moving a user's files from one device to another), or may be manually transferred from an "old" computer to a "new" computer. In my experience in digital investigations, it is common to find data and files on a computer that are older than a computer itself (e.g., photographs and video files dated before the "new" device was manufactured, transferred from an "old" device to a "new" device).

52. Where the crux of a search is for child pornography currently possessed by an individual - that is digital images and video - the target's primary computer, typically the one used to access the internet, is but one container to search. The ease by which digital files can be transferred and ubiquity of low-cost digital storage allow for many devices on which child pornography can potentially be stored. Further, I know from my training and experience that collectors of child pornography, knowing that they possess contraband, can be creative in their storage and secreting of child pornography - which in the past has included secreting removable storage media inside of a home, and maintaining old internal hard drives that are no longer inside of computers.

53. Where the search is also for evidence of past access to child pornography, forensic analysis of seized computers can reveal evidence through data that is both apparent and non-apparent. Manual review of a computer, or use of a forensic tool, may quickly reveal apparent evidence of past access to child pornography, whether months or years ago. For example, logs showing access to child pornography websites, or saved web addresses of child pornography websites would be this type of evidence. On the other hand, forensic analysis may also reveal non- apparent data, data that had been deleted or obfuscated by a user. Forensic tools may be able to recover data deleted months or even years ago, including photographs depicting child pornography. Forensic tools may also be able to recover data showing past access, and ongoing access, to child pornography websites, even if files were not intended to be downloaded by a user (e.g., the user viewed child pornography on a website but did not overtly take efforts to download the image file). For example, photographs viewed on a website may be stored a "thumbnail" images on a computer, without the user knowing that they are stored, showing prior access to a child pornography website months or years ago.

54. In my experience with HSI, I know that HSI investigators have been involved in child pornography investigations where evidence of access and possession of child pornography was forensically recovered from computers and the data was over 5-years-old.

55. I believe a search of the TARGET PREMISES, and analysis of computers contained therein, will reveal child pornography, and evidence of a user's access to the CP Website among other child pornography websites.

USE OF COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

56. As described above and in Attachment B, this application seeks permission to search for records that might be found on the TARGET PREMISES, in whatever form they are found, including data saved to computers. One form in which the records are likely to be found is

data stored on a computer's hard drive or other electronic storage media. Thus, this warrant would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, under Rule 41(e)(2)(B).

57. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on a device. This information can sometimes be recovered with forensics tools.

58. *Forensic Evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of violations of the TARGET OFFENSES, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on computers found in the TARGET PREMISES because:

a. Data on the electronic storage media may provide evidence of a file that was once on the electronic storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the electronic storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the electronic storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, such as the attachment of USB flash storage devices or other electronic storage media, and the times the computer was in use. Computer file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be altered or falsified by a user.

b. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage media until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the electronic storage media that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but most computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." An Internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information logs which may reveal:

i. computer user account session times and durations;

ii. computer activity associated with user accounts;

iii. electronic storage media that connected with the computer;

iv. and the IP addresses through which the computer accessed networks and the Internet;

f. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both depict a particular location in a photograph and have geolocation information incorporated into its file data (e.g. a photograph clearly taken at City Hall in Burlington, Vermont with GPS coordinates of the location in Burlington where the photograph was taken incorporated into the photograph's metadata). Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage

media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user.

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on an electronic storage media, necessary to draw an accurate conclusion, is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on an electronic storage media. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

59. I know that when that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, contain data that is evidence of the crime, and serve as storage media for fruits of the crime (e.g., contraband child pornography). The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be electronic storage media for evidence of crime.

From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

Necessity of Seizing or Copying Entire Computers or Storage Media

60. Based on my knowledge, training, and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence - storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.

b. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is

exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

c. Technical requirements - analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence, and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

61. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

62. The TARGET PREMISES may contain computer equipment whose use in the TARGET OFFENSES or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this

warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

63. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

Nature of Forensic Examination

64. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

65. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records, and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or

disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

66. It is possible that the TARGET PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

67. *Manner of execution.* This warrant seeks only authorization to execute the search of the TARGET PREMISES during the day time – that is 6:00a.m. to 10:00p.m., local time.

CONCLUSION

68. Based on the foregoing, I submit that there is probable cause to believe that violations of the TARGET OFFENSES have been committed at the TARGET PREMISES. Since there has been no change of subscriber, William KEVE, to IP address 69.5.116.44 at the TARGET PREMISES since before someone accessed the now-defunct CP Website, and the current subscriber, William KEVE, still receives mail at the TARGET PREMISES, I believe there is probable cause that, based on the knowledge of how persons interested in viewing, exchanging, and collecting child pornography often keep their collections for months and years, that stored computer media may never truly be deleted from an electronic storage device, and that access to the CP Website took significant knowledge and intent, evidence of the TARGET OFFENSES still exists at the TARGET PREMISES. I respectfully submit that there is probable cause that the contraband, property, evidence, fruits, and instrumentalities of the TARGET OFFENSES, more fully described in Attachment B of this Affidavit, including child pornography and digital evidence of continued access to child pornography using the Internet, are located at the TARGET PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the TARGET

PREMISES described in Attachment A, authorizing the seizure and search of the items, including computers, described in Attachment B.

Respectfully submitted,

Seth M. Fiore
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on Dec. 4th, 2020

HON. JOHN M. CONROY
UNITED STATES MAGISTRATE JUDGE